УДК 004

К. А. Шолоков
курсант 2-го курса факультета милиции
Могилевского института МВД
(Беларусь)

А. С. Мойсевич
преподаватель кафедры оперативно-розыскной деятельности
факультета милиции
Могилевского института МВД
(Беларусь)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ WI-FI

В настоящее время существует много технологий и способов передачи информации. И все чаще для ее передачи применяются беспроводные сети, отличающиеся от других тем, что вместо сетевого кабеля и коммутаторов в них применяются преобразователи среды, которые передают информацию в эфир, предварительно преобразовав ее в радиоволны. Радиоволны поступают на приемник, который обратно преобразует их в информацию.

Существуют различные виды беспроводных сетей, однако особое место среди них занимают беспроводные сети, основанные на технологии Wi-Fi. К примеру, сети Wi-Fi часто используют пользователи услуг электросвязи для домашнего доступа к Интернету [1, с. 12–43].

Специалистами по кибербезопасности отмечено, что злоумышленники, подключающиеся к незащищенной домашней сети Wi-Fi, могут получить персональные данные пользователей, проанализировав передаваемые ими по сети данные. В связи с этим для пользователей домашней сети, работающей по технологии Wi-Fi, ими разработаны общие рекомендации по обеспечению ее безопасности [2].

1. Изменение пароля администратора. Точка доступа Wi-Fi, как правило, ставится с паролем по умолчанию для учетной записи администратора, который позволяет изменять конфигурацию устройства. Часто эти пароли по умолчанию общеизвестны, зачастую даже размещены в Интернете с указанием конкретной модели роутера. Поэтому пользователю услуг беспроводной сети необходимо в обязательном порядке изменить пароль администратора на уникальный, надежный, чтобы только у клиента (пользователя) был к нему доступ. Если устройство позволяет это сделать, также следует изменить и имя пользователя [2].

2. Создание сетевого пароля. Клиенту необходимо настраивать домашнюю сеть Wi-Fi так, чтобы она также имела уникальный и надежный пароль. Таким образом, только люди и устройства, которым доверяет пользователь, могут присоединиться к его домашней сети. В этой связи специалистами рекомендуется рассмотреть возможность использования менеджера паролей для выбора более надежного пароля [2].

3. Обновление встроенного программного обеспечения. Включение автоматического обновления операционной системы точки доступа Wi-Fi, часто называемого встроенным программным обеспечением, гарантирует максимальную безопасность устройства с помощью имеющихся новейших средств защиты. Если автоматическое обновление не предусмотрено в точке доступа Wi-Fi, периодически пользователю необходимо входить в систему и проверять устройство, чтобы узнать, доступны ли какие-либо обновления. Если устройство больше не поддерживается поставщиком, рекомендуется приобрести новое, которое можно обновлять и получать новейшие функции безопасности [2].

4. Использование гостевой сети. Гостевая сеть — это виртуальная отдельная сеть, которую может создать точка доступа Wi-Fi. Это означает, что точка доступа Wi-Fi фактически имеет две сети. Основная сеть — это сеть, к которой подключаются надежные устройства, такие как компьютер, смартфон или планшетные устройства пользователя. Гостевая сеть — это то, к чему подключаются ненадежные устройства, к примеру, устройства гостей, посещающих дом, или, возможно, некоторые из персональных устройств умного дома. Когда что-то подключается к гостевой сети, оно не может видеть или взаимодействовать ни с одним из надежных персональных устройств, подключенных к основной сети [2].

5. Использование безопасной фильтрации DNS. DNS — это интернет-сервис, который преобразует имена веб-сайтов в цифровые адреса. Это то, что помогает гарантировать, что компьютер сможет подключиться к веб-сайту, когда вводится имя веб-сайта. Точки доступа Wi-Fi обычно используют DNS-сервер по умолчанию, предоставляемый провайдером, но более безопасные альтернативы доступны бесплатно в таких службах, как OpenDNS, CloudFlare для семей или Quad9, которые могут обеспечить дополнительную безопасность, блокируя вредоносные или другие нежелательные веб-сайты [2].

Подводя итог изложенному, отметим, что защита домашней точки доступа Wi-Fi — это первый и один из самых важных шагов в создании безопасной сети. Обеспечение безопасности сети требует постоянства и пристального внимания к деталям. Это заключается в предсказании возможных действий несанкционированных действий, принятии мер защиты, постоянном изучении рекомендаций по безопасности пользователем.

1. Технологии современных беспроводных сетей Wi-Fi : учеб. пособие / Е. В. Смирнова [и др.] ; под общ. ред. А. В. Пролетарского. М. : Изд-во МГТУ им. Н. Э. Баумана, 2017. 446 с. Вернуться к статье

2. Joshua Wright. Securing Wi-Fi at Homehttps [Electronic resourse] / SANS. URL: www.sans.org/newsletters/ouch/securing-wi-fi-home/ (date of access: 30.09.2021). Перейти к источнику Вернуться к статье